

ملحق(E)

المواصفات الفنية للخدمات المدارة

NVR- 64 Channels IVS1800 (qty 1 per PHC site)

- Supports 64-channel video access, storage, and forwarding, with a maximum access bandwidth of 160/256/320 Mbit/s (160 Mbit/s when intelligent analysis is enabled).
- Features no more than 2 U chassis with at least eight disk trays and supports 4/6/8/10/16 TB hard disks.
- Provides two HDMI ports, one VGA port (extended using an external conversion cable), one audio-in/out port, four Boolean input ports, and two Boolean output ports.
- Target analysis: Supports 4-channel 1080p video-based (or 12 1080p images per second) target analysis, including real-time target feature extraction, blocklist/trustlist-based target alert, target search by image, masked target recognition, and mask alarm.
- Video-based pedestrian analysis: Supports 2-channel video-based personal attribute recognition, including gender, age group, tops color, bottoms color, tops pattern, tops style, bottoms style, hand-held objects, glasses, backpack, crossbody bag, hairstyle, hat, umbrella, mask, posture, physique, luggage, and holding objects.
- Supports 2-channel perimeter detection, including tripwire-crossing detection, intrusion detection, area entry detection, area exit detection, loitering detection, and abnormal speed detection.
- Supports target, person, behavior analysis algorithms and third-party long-tail algorithms (concurrent running of three algorithms and concurrent analysis of video and images are supported).
- Supports person, behavior analysis algorithms and third-party long-tail algorithms, and supports concurrent running of up to three algorithms.
- Supports concurrent analysis of video and images
- Supports southbound camera access through GB/T 28181 and ONVIF
- Supports connection to upper-level platforms as a device through GB/T 28181 or ONVIF
- Supports SafeVideo+
- Supports various encoding formats (H.264, H.265, MJPEG, and more)
- Supports hybrid storage of video and images
- Supports video buffering, ensuring video data integrity
- Supports to embedded Linux operating system, ensuring 24/7 stable running and protecting the system from hackers and viruses
- Supports status indicators, facilitating device and disk maintenance
- Supports free of system disks and available upon device startup
- Supports recording mode: Manual recording, scheduled recording, and alarm-triggered recording
- Support multiple encryption algorithms such as AES256 are supported for data transmission
- Support digital watermarks can be added to video from cameras. Alarms are generated when video is tampered with
- Support two copies of key system data are stored. If a fault occurs, service data can be automaticallyrestored.
- Store 2 video streams of cameras for 30 days, one is 1080P for live view, and another one is 720P for backup to central platform.
- Support 5 Years Vendor Support 9*5 NBD



Central CCTV Storage - IVS 3800 (Access Node + Storage Node) (qty- 8)

Two types of CCTV cluster nodes need to be deployed on the central side.

- Access Nodes will manage all video access from NVRs of each branch and back up these data to storage nodes
- Storage Nodes will help to saving all video data for 90 days

The two types of nodes cooperate with each other to achieve the following functions and features

- Software Specification
  - The system shall support user management, device management, device connection, external domain platform connection, and video/image storage and forwarding.
  - The system shall be able to directly obtain configurations of the automatically discovered ONVIF-compliant devices to implement services such as live video viewing.
  - The system shall allow users to play a specified live stream if a camera supports multiple streams.
  - The system shall support multiple encoding formats such as H.264 and H.265.
  - The system shall support video buffering. When cameras are disconnected from the network, the cameras can continue to shoot video and temporarily store the video in SD cards. When the network is recovered, the platform shall send a video request to the cameras. The cameras then send the video stored in SD cards to the platform.
  - The system shall support statistics over the online rate, offline rate, status, recording integrity, packet loss rate, and SD card faults of video devices. The system shall be able to display the statistics in charts and allow users to export the statistics into Excel files.
  - The system must support Raid 5 or EC (Erasure Coding) as data protection technology

    a)Raid 5:
    · Support 1 to 3 RAID5 groups for one server with hot spare disks and support service migration among RAID groups upon faults.
    · Allow data to continue being written into and read from the faulty RAID 5 group. Video read from the faulty RAID group can be basically viewed.
    b)EC:
    · EC data protection with +2 EC ratio is supported
    · Large-ratio EC of 22+2 is supported.
  - The system shall support management of cluster node services throughout the lifecycle, including cluster software deployment, cluster node service setup, expansion, startup, stop, and deletion, and cluster dismissal. The system shall allow the storage space on multiple nodes to form a unified storage space and provide services for external systems using the same IP address. The system shall support storage load balancing among multiple nodes and preferential access to the neighboring node.
  - The system shall allow users to view cluster information on web pages, including the cluster storage space, disk status, member status, and recording plan status.
  - The system shall support the N+0 cluster. Storage nodes in a single cluster do not need an independent cluster management server. When any node is faulty, services on the faulty node can be migrated to other nodes.
  - The N+0 cluster feature can automatically schedule video and image services without the need for an independent backup server. Users need to add and configure cameras only once.



- After a service unit (service module or cloud node) recovers, the system shall migrate some services on other service modules to the recovered service unit. When a service module is overloaded, the system shall migrate some services on this service module to other service units.
- The system shall be able to collect statistics on the number of video stream requests, number of image stream requests, number of online devices, number of offline devices, number of times that cameras in a cluster are migrated to or out of a node, number of server snapshots, number of recording requests, and number of connected external domain devices. The system shall support display and real-time refresh of KPI monitoring data in charts and tables, and allow users to search for data generated in the past hour, past 12 hours, past day, past 3 days, past 7 days, or by custom period.
- The system shall be able to back up images and key data to data disks and generate multiple copies. Key data includes data related to system operations such as the database data, configuration files, and recording index files. The system shall support data restoration by reading backup data from data disks upon faults.

- Hardware specification---(Access Node)
  - At least two 32-core processors with a clock rate of at least 2.6 GHz shall be configured.
  - The memory must be greater than or equal to 64 GB and use DDR4 or higher specifications.
  - The device shall be installed in a 19-inch standard rack. The device shall adopt cable-free modular design with independent main control module, hot-swappable hard disk, and power module.
  - Two independent system disks shall be configured to form RAID 1.
  - The system shall support power modules in 1+1 redundancy mode and independent maintenance of power modules.
  - Single Node can support a maximum of 1200 - channel video access and forwarding with 2 Mbps Camera bandwidth at same time
- Hardware specification---(Storage Node)
  - At least two 32-core processors with a clock rate of at least 2.6 GHz shall be configured.
  - The memory must be greater than or equal to 64 GB and use DDR4 or higher specifications.
  - The device shall be installed in a 19-inch standard rack. The device shall adopt cable-free modular design with independent main control module, hot-swappable hard disk, and power module.
  - A single device shall support at least 33 enterprise-class disks, with single disk supports 8 TB/10 TB/16 TB capacity.
  - The system shall support soft start of hard disks.
  - The system shall support SATA disks and support hot swap and online replacement of faulty disks.
  - Two independent system disks (SSD of 960GB) shall be configured to form RAID 1.
  - Onboard 4 x GE (Electrical port) + 2 x 10GE optical ports
  - The system shall support four independent fans and work properly when a single fan fails.
  - The system shall support power modules in 1+1 redundancy mode and independent maintenance of power modules.
  - Single Node can support a maximum of 1200 - channel video access and storage with 2 Mbps Camera bandwidth at same time.
- Integration specification
  - The system shall provide the device connection gateway and support the SDK, ONVIF protocols.
  - The system shall provide HTTP-based RESTful APIs for ISVs to integrate service functions such as live video viewing, PTZ controls, recording search and playback, backup, alarming, voice intercom, recording download, and snapshot taking.
- Support 5 Years Vendor Support 9*5 NBD



Decoder (qty- 2)

- Decoder should support 8 channels HDMI port
- Decoder should support Video output through HDMI 1024×768P@60Hz,1280×720P@60Hz, 1366×768P@60Hz,1920×1080P@60Hz, 3840×2160@60Hz
- Decoder should support H.264, H.265
- Video decoding capacity supports 8CH 4K or 64ch 1080P or 128ch 720P or 256ch D1
- Screen division support 1/4/6/8/9/10/16/25 splitting and display
- Network port One RJ45 100/1000 Mbit/s self-adaptive Ethernet port
- Support 5 Years Vendor Support 9*5 NBD

VMS Specification

- The VMS should support multi-level, multi-domain, and multi-node based on the organizational structure and cross regional distribution characteristics of headquarters and branches, the hierarchical relationship should be highly abstract to form a set of organizational management rules
- The VMS should support an open architecture of middleware, adapt the concept of microservices architecture for design, and shield variant technical details through software interfaces for future system upgrades and expansion
- The VMS should have technical features such as strong compatibility with heterogeneous devices, interconnection and control of heterogeneous platforms
- Optimize the file system for scenarios such as real-time video data, large data volume, and cyclical deletion, using file system metadata and media data analysis modes
- Establish a hot backup data center in a different location for data backup through the network This means backing up the data from the primary site to the disaster recovery site through the network in a synchronous or asynchronous manager When problems occur at the primary site, the backup site takes over the business of the primary site, they maintain the continuity of business operations
- The system should support the configuration of floating virtual IPs for the primary and backup node gateways to achieve hot switching between the gateway and the backup node
- Support the output of real-time video streams or recorded video streams using the RTSP protocol and HTTP+FLV protocol real-time video streams or recorded video streams; Support IPSAN, NAS, and OBS object storage (supporting S3 interface) and other forms
- Support access to camera devices through the ONVIF protocol
- Support the distribution of real-time video streams from front end cameras to VMS clients for playback
- Users can view different perspectives and details through PTZ while conducting real-time browsing PTZ control operations include: direction control (up, down, left, right, top left, bottom left, top right, bottom right), lens control (zoom, magic, iris), preset position, and guard position
- Support user defined addition of alarms, including alarm level names, alarm weights, and alarm types Support alarm type query, presented in accordance with the painting, can view the details
- Support for loading electronic maps, adding cameras on to the map, displaying cameras on the map based on camera latitude and longitude information
- Support for different user roles view the camera settings, different users set different camera access rights, if the user does not have access rights to a particular camera, the user will not be able to view the camera
- Configure the video policy, support the configuration of scheduled video, alarm video, manual video retention period, support the configuration of the video code stream, distinct between ordinal video and alarm video using the code stream



- Support querying user operation logs and system alarm logs according to conditions, and displaying them in the form of a list.
- VMS supports the restart and stop of application modules VMS supports the monitoring of archive information management and operation status. VMS archive information management includes platform server, database, middleware and other information. Operation status monitoring includes the operation rate of various system components (disk occupancy, memory occupancy, load value, operation status, etc.).
- VMS statistical analysis module is divided into resource statistics and report customization. It performs statistical analysis on video and analysis data of various dimensions of resources, classifies statistics according to various dimensions, displays the results of operation status, manages operation and maintenance evaluation, and counts resource status.
- Online appraisal reports can be queried by date. You can query and export the organization's quantity to be linked, actual linked quantity, access rate, total number of patrols, online number of patrols, online rate of patrols, and score status.
- It supports the statistics of image quality integrity detection of assessment equipment at all levels according to the time period, forming statistical data and presenting it in a graphical manner, so that customers can view historical statistical information and master the overall operation.
- VMS makes accurate judgment on camera video image failures, such as image color deviation, interference noise, snowflake noise, signal loss, definition failure, brightness failure, image freezing, scene transformation, artificial occlusion and the severity of failures, automatically records all detection results and reports them to the monitoring management center.
- Support 5 Years Vendor Support 9*5 NBD

Central platform for network management and monitoring and Authentication



الكمية	الوحدة	الصنف	البند
		متطلبات تشغيل وإدارة الشبكة من مركز البيانات لدى مزود الخدمة	
2	أجهزة وبرمجيات	Huawei Wi-Fi Controller Platform with Licenses and Support for 5 years	1
3	أجهزة وبرمجيات	Huawei Wi-Fi & Switch Management Platform with Licenses and Support for 5 years	2
3	أجهزة وبرمجيات	Huawei Wi-Fi User Analyzer and O& M Platform with Licenses and Support for 5 years	3

1.1 **Wi-Fi Controller**
Technical Specifications
• Supports High Availability features for maximum operations for the system
• The Device should support to be managed by a Wi-Fi Management Platform to obtain a converged and intelligent solution
• Supports up to 6000 Access Points
• Supports up to 120 Gbit/s forwarding performance (Direct & Tunnel Forwarding)
• Supports up to 32K Users
• Supports 12 x 10GE optical interfaces and 12 x GE electrical interfaces
• Supports Load balancing during smart roaming



• Supports Intelligent DFA technology
• Supports Intelligent conflict optimization technology
• Supports 802.11 a/b/g/n/ac/ax & 802.11be
• Can be deployed in inline, bypass, bridge, and Mesh network modes
• Supports both centralized and local forwarding
• Supports AC and APs can be connected across a Layer 2 or Layer 3 network
• Supports Layer 4 to Layer 7 application identification
• Supports application-based policy control technologies
• Supports redundant and hot swappable power supplies
• Supports WLAN AC 1+1 HSB, and N+1 backup
• Supports Link Aggregation Control Protocol (LACP)
• Supports Multiple Spanning Tree Protocol (MSTP)
Supports Jumbo frames
Supports Static, dynamic, and blackhole MAC address entries
Supports Static and dynamic ARP entries
Supports LLDP
• Supports BPDU protection, root protection, and loop prevention
• Supports ARP and RARP
• Supports RIP-1 and RIP-2, OSPF, BGP and IS-IS
• Supports IGMPv1, IGMPv2, and IGMPv3, PIM-SM
• Supports RIPng, OSPFv3, BGP4+ and IS-IS IPv6
• Supports 802.1p priority
• Supports SNMPv1, SNMPv2c, and SNMPv3
• Supports RADIUS authentication
• Supports SSHv2.0
• Supports Centralized CAPWAP
• Supports IoT cards on the AP to converge the WLAN and IoT
• Supports intra-AC Layer 2 roaming
• Supports built-in Portal/AAA server
• Supports Portal/802.1X authentication
• Supports WPA and WPA2 encryption
• Supports Up to 8K MAC Address
• Supports up to 8K IPv4 Routes



	• Supports Direct forwarding, Tunnel forwarding and Tunnel forwarding + EoGRE tunnel
• Include 5 Years Vendor Support 9*5 NBD	

1.2 Wi-Fi Authentication and Management Platform ((Hardware, Software& Licenses)	
	Technical Specs and Requirements
Key Feature	**Description**
	Wi-Fi Authentication and Management Platform is next-generation autonomous driving network management and control system for campus networks. It should be first-of-its-kind intelligent network automation platform which integrates management, control, and analysis functions, provides full-lifecycle automation of campus networks, and implements intelligent fault closure through big data analytics. These innovative features help enterprises reduce OPEX and O&M costs, accelerate enterprise cloudification and digital transformation, and achieve automated and more intelligent network management.
	As the intelligent management and O&M center of the campus network, Platform should cover large- and medium-sized campus networks and multi-branch interconnection networks. It should have the following key capabilities:
	• Automatic network deployment: physical network deployment automation, virtual network service provisioning automation, and LAN-WAN converged management.
	• Service policy automation: mass user authentication, intelligent terminal management, 5G terminal access, IoT sensing network, and hierarchical QoS scheduling.
	Intelligent O&M: real-time experience visibility, fault locating in minutes, and intelligent network optimization
Simplified Network Deployment	• Provides four PnP deployment modes: deployment through app-based barcode scanning, Simplified deployment through DHCP, deployment through the registration query center, deployment Network through the email and ZTP-based deployment, to adapt to different network Deployment scenarios.
	• GUI-based network planning and deployment and provision network services in minutes.
Automatic Virtual Network Service Provisioning	■ Visualized service configuration and GUI-based fabric planning, configuration, and provisioning.
	■ Automatically establish VXLAN tunnels through BGP EVPN.
	■ Supports centralized and distributed VXLAN gateway solutions, providing flexible expansion and high efficiency
	■ Supports service configuration visualization, topology-based virtual network configuration and monitoring, and real-time service provisioning status query.



User Access Authentication	Introduces new authentication protocol HTTP2.0, and can authenticate a large number of network devices and users using various access authentication modes, such as 802.1X authentication, Portal authentication, SMS authentication, and social media authentication.
	Provides the 5G terminal access authentication capability, ensuring that 5G terminals can access enterprises 'campus networks in a secure and reliable manner.
	Users decoupled from IP addresses, allowing users to access the network anytime, anywhere with consistent permissions. This ensures free mobility and consistent user experience, ensuring user experience while meeting permission control requirements.
Multi-tenant Management	■ Adopts a three-level management model: The system administrator is responsible for platformwide management and O&M. The MSP administrator can create tenants and provide construction and maintenance services for tenants. The tenant administrator is responsible for deployment and
	■ O&M of the local network; alternatively, the tenant administrator can authorize an MSP to manage tenant networks.
	■ Management • Supports rights- and domain-based management. In the three-level management model, administrators can be set by role and site to secure network management.
	■ Services are invisible between tenants. Data of different tenants is isolated in an E2E mode and distinguished by tenant IDs in the database. In addition, only the corresponding tenant Administrator can access data of a tenant. This ensures tenant data security to the most extent.
Intelligent Terminal Management	• Built-in terminal fingerprint library: Multiple intelligent identification methods are combined to accurately identify endpoint types.
	• Massive IoT endpoints are connected intelligently, and policies are automatically matched and delivered, making IoT endpoints plug-and-play.
	•The IoT sensing network simplifies and improves the security of IoT terminal access.
	•AI clustering forun known terminal identification:Unknown terminals with similar fingerprints are clustered into one group, and then the administrator marks the terminal type.These unknown terminals then can be automatically identified.
Intelligent	• HQoS scheduling based on users and service priorities: Different policies are implemented for different users and applications, achieving more refined bandwidth policy control and effectively ensuring user access experience.
HQoS	
Intelligent O&M	• Provides networking monitoring, network inspection, and health evaluation to monitor device alarms in real time and detect network conditions in advance for fault prevention. If a fault occurs, Platform provides various fault locating methods to quickly locate and rectify the fault.
	• Real-time experience visibility for each application of each user in each area: With fault backtracking, Platform quickly and intelligently demarcates faulty devices and analyzes root causes for poor quality.



	• Continuously trained algorithm: Through proactive issue identification, fault locating in minutes, and intelligent fault prediction, Platform identifies 90% of potential network faults and provides optimal rectification suggestions.
	• Real-time wireless network channel conflict evaluation: Platform performs predictive radio calibration, and compares gains before and after calibration, improving network performance by more than 50%.
Capability Openness	• Provides 170+ northbound RESTful APIs for user management, topology management, access authentication, service configuration, and performance monitoring.
Hardware , Software & Licenses Management Capacity and Performance	Required Hardware Servers configuration: Three nodes (Servers) –
	(2*16Core/2.3GHz CPU,4*32G Memory,4*1200GB SAS HDD,RAID(2G cache)+SuperCap, 2*4*GE+2*10GE SFP+,2*900W AC). Include 5 Years Vendor Support 9*5 NBD
	OS Linux & Database.
	Licenses for Wi-Fi APs and Authentication

1.3 Wi-Fi Network Analyzer Platform (Hardware & Software)

	Technical Specs and Requirements
Feature	**Description**
Multi-dimensional network status visualization and client experience awareness throughout the journey	• Displays multi-dimensional data statistics views based on different levels and regions.
	• Supports user-defined views and displays key statistics information about networks and users on the screen in carousel mode.
	• Displays issues about network access, network congestion, device status, and error packets from the perspective of buildings.
	• Searches users from the perspective of buildings and displays information about buildings that users passed by in a specified period of time.
	• Allows administrators to import topology views and plan AP locations to intuitively view fault location distribution.
	• Automatically discovers the topology corresponding to the physical network, displays the network information in the topology view, and monitors the entire network in real time.

	• Displays the radio heatmap by AP location.
	• Allows administrators to import network planning data to be compared with the actual network running data, displaying the differences between them.
	• Allows administrators to view the full-journey experience, including who, when, which AP to connect, experience, and issues.
	• Supports device profiles and allows administrators to view the health status of switches, APs, and routers.
	• Displays spectrum analysis results based on APs, including full-channel status monitoring, Wi-Fi interference sources, and non-Wi-Fi interference sources.
	• Generates dialing test reports for multi-vendor network comparison in real time and allows administrators to intuitively learn the Wi-Fi network experience through dialing tests on apps.
	• Traces the network access process of a client, including detailed protocol information at the association, authentication (supporting 802.1X authentication, Portal authentication, MAC address authentication, HACA authentication and PSK authentication), and DHCP phases. The protocol information includes the interaction result and time used. If the interaction fails, the failure causes are also displayed.
	• Correlatively analyzes poor-experience clients. When the experience of a client deteriorates, CampusInsight identifies quantified correlation KPIs based on the KPI similarity analysis algorithm, which effectively improves the accuracy of root cause identification.
Automatic identification and proactive prediction of network issues	• Supports automatic identification of common network issues based on big data analytics and ML algorithms: connectivity, air interface performance, roaming, device environment, device capacity, network performance, network status, and network protocol issues. The issues include authentication failure, weak-signal coverage, dual band-capable clients prioritizing 2.4G, and network congestion.
	• Supports learning and dynamic baseline drawing on network behavior to predict the change trend and detect exceptions through data comparison.
	• Intelligently analyzes data reported at the second level and establishes a network health evaluation system from multiple dimensions. CampusInsight evaluates and ranks regions based on indicator weights, driving continuous improvement from poor experience to good experience and gradually improving the network quality. The dynamic baseline comparison between the local region and other regions for each indicator can be viewed. CampusInsight provides associated root cause indicators, enabling in-depth root cause analysis. Different time or areas can be selected for comparison and analysis and sends network health reports are sent to the administrators in real time or periodically by emails.
	• Establishes roaming baselines based on different terminal types, intelligently determines the optimal roaming time, and provides users with intelligent and lossless roaming experience.



Intelligent demarcation and root cause analysis of network issues	• Supports the issue distribution view, allowing administrators to view the number of issues on different devices and the number of affected clients. This helps administrators quickly focus on the affected devices where and the time range.
	• Supports issue impact analysis views, allowing administrators to filter impact factors from multiple dimensions and drill down layer by layer to quickly locate the issue root cause.
	• Analyzes the root causes and provides rectification suggestions to assist quick issue closure.
Open northbound APIs, providing various data for	· Supports different secondary development capabilities based on data characteristics. Three types of interfaces can open the raw data and analyzed data to third-party systems, including network O&M and IT service systems, thereby offering richer intelligent analysis data.
intelligent analysis	(1) RESTful NBI: opens resource data (device, interface, link, and board data), health data (health issue and health evaluation data) and terminal session data to external systems.
	(2) SNMP NBI: reports alarm data to a third-party system through SNMP.
	(3) Kafka NBI: consumes data collected by CampusInsight using Telemetry through the consumer API provided by Kafka.
Analyzer Hardware - Management Capacity and Licenses	Required Hardware Servers configuration: Three nodes (Servers) –
	(2*16Core/2.3GHz CPU,8*32G Memory,8*1200GB SAS HDD,9460-8i(2G cache)+SuperCap,2*4*GE+3*2*10GE,2*900W AC). Include 5 Years Vendor Support 9*5 NBD
	OS Linux & Database & Licenses for all Wi-Fi AP

1.5 Network Management System (Hardware, Software & Licenses)

Indicator	Technical Specifications
Management scale	The system can support large-scale device management. A maximum of 20,000 NEs can be managed.
Management scope	The system can manage multiple types of devices, including switches, routers, firewalls, WLAN devices, servers, storage devices, HCI, OS, Database, Web Application, cameras, GPON and CPE devices.
System architecture	The system can support mainstream browsers such as Internet Explorer, Firefox, and Chrome based on the B/S architecture.
System security	The system can provide the rights- and domain-based management function to assign different device management scopes and operation rights to different users and roles.
	The system can support local, RADIUS, LDAP and OAuth2.0 user authentication management to implement centralized user management.



	The system can provide system logs, operation logs, and security logs.
System openness	The system can open three types of northbound interfaces (SNMP, FTP, RESTful and Message queue) to provide alarm, performance, and resource data to the upper-layer system.
	The system can support multiple types of southbound interfaces, including SNMP, STelnet, FTP, SFTP, IPMI, HTTP/HTTPS（REST/Redfish）, LwM2M, WebSocket, SocketPing, ICMP, WebPing, WebTrace and SSDP interfaces to manage multiple types of devices.
Resource management	The system can support resource management by group. Resources (such as servers, network devices, and storage devices) connected to eSight can be managed by type or group. Users can create group types and groups to manage resources.
	The system can provide the link management to display links between devices, view conflicting links and link discover, monitor and configuration are supported.
	The system can support the power-on and power-off management, servers and storage devices connected to NMS can be remotely powered on or off.
Topology management	The system can support to build and manage the topology of the entire network to reflect the networking and running status of NEs. Users can monitor the running status of the entire network in real time in the topology view.
	The system can support physical topology, a topology view that displays NEs, links, and subnets on the entire network.
	The system can support customized topology, a cross-subnet topology view that displays NEs and links on part of the entire network. O&M personnel can customize a topology with the managed NEs to understand how these NEs are deployed across subnets and precisely monitor the NEs.
	The system can display the alarm status of NEs and links in topology views and support basic operations such as device information viewing, device status, alarms and KPIs.
Fault management	The system can support to collect data from multiple domains and vendors, including NE alarms from third-party systems, and the alarms are displayed on the alarm panel.
	The system can provide diversified alarm filtering methods, which enable O&M personnel to filter concerned alarms and improve monitoring efficiency.



	The system can enable flexible alarm rule configurations to associate and compress a large number of alarms, reducing alarm noises and achieving precise monitoring.
	The system can categorize alarms into critical, major, minor, and warning, helping O&M personnel quickly identify alarm severities and implement corresponding handling policies.
Performance management	The system can monitor key performance indicators of devices and collect statistics on obtained performance data to facilitate device performance management.
	The system can generate alarms of four levels (critical, major, minor, and suggestion) by setting different performance thresholds.
	The system can allow users to view the historical performance data of a specified device or indicator to learn about the historical performance trend.
	The system can monitor the real-time performance data of devices so that users can learn about the running status of the devices and check whether the devices are abnormal. The system can export the query result to an EXCEL file.
Report management	The system can allow users to customize reports in drag mode and support data drilling, rotation, and slicing to flexibly display and summarize service data. The system can provide functions including self-service data comparison, chain comparison, and Top N statistics.
	The system can automatically generate reports in periods specified by users and send reports by email or allow users to manually export reports in EXCEL, PDF, WORD or HTML formats.
Network resource management	The system can provide an integrated dashboard of network devices (including switches, routers, firewalls, and ACs). This dashboard displays key information, such as devices, components, simulation panels, and running statuses, helping O&M personnel quickly learn about devices, identify, locate, and rectify device faults.
Network report template	The system can display information in reports, such as alarms, performance, wired and wireless resources, and user terminal location information.
Configuration file management	The system can manage the configuration files of the devices on the entire network, back up the configuration files in real time and periodically, and baseline the backup file for configuration restoration and comparison.
Network configuration management	The system can deliver configurations in batches in two modes, that is user customize template and command planning table.



Device Software Management	The system can upgrade software version and install software patch in batches for network devices, including routers, switches, and firewalls.
Network quality monitoring	The system can proactively send diagnosis packets between network devices based on the NQA protocol to measure KPIs, such as the packet loss rate, delay, and jitter.
	The system can support various monitoring modes, including ICMP Echo、ICMP Jitter 、UDP Echo、UDP Jitter、DNS and DHCP
Network Traffic Analysis	The system can monitor network-wide traffic in real time and provide multi-dimensional top n traffic analysis reports, helping users detect abnormal traffic on the network and network bandwidth usage in time.
	The system can offer drill-down network traffic analysis for users to view traffic details by criteria. Top *N* traffic analysis can be performed by link interface, application, host, session, or device.
WLAN management	The system can support docking with mainstream planning tools, and can quickly import network planning data, simulate building, floor and obstacle planning, and realize visible signal coverage.
	The system can support dashboard O&M of WLAN network, including overview, top AP statistics, traffic trend, user trend, top regional statistics, etc.
	The system can support WIDS management, detect illegal devices / clients, interference sources and attacks in WIFI network, and notify O&M personnel through alarm.
	The system can support one click fault detection, identify problems from seven dimensions of terminal, SSID, AP, AC, connectivity, AAA and DHCP, and provide fault causes and repair suggestions.
	The system can provide radio report, AP interface report, AC join statistics report, AC traffic detail report, AC user trend report, AP join detail report, AP load detail report, AP uptime report, AP traffic detail report, STA client detail report, STA online client detail report at least.
IP address Management	The system can support the overview of IP address statuses, manage IP address groups, or plan IP subnets. Users can manage IP addresses and subnets by group, assign, or reclaim IP addresses.
NMS - Hardware , Software & Licenses Management Capacity and Performance	TaiShan 200 (Model 2280) Outside(2*Kunpeng 920-48Core@2.6GHz CPU,4*32GB Memory,2*1920GB SSD,Raid(2G cache,SuperCap),8*GE,2*900W AC) Include 5 Years Vendor Support 9*5 NBD



	Operating System (OS) & Database & Licenses for all Wi-Fi AP & Switches